IDENTITY THEFT PREVENTION
SDPD Neighborhood Policing Resource Team
April 5, 2013

CONTENTS

This paper contains tips for preventing identity theft. Additional tips on cyber security, fraud prevention, personal safety and security, home and vehicle security, vacation safety and security, senior and child safety and security, and preventing crimes against businesses can be found on the prevention tips page of the SDPD website at **www.sandiego.gov/police/services/prevention/tips/index.shtml**.

Every person who willfully obtains personal identifying information, e.g., name, address, date of birth, Social Security Number (SSN), mother's maiden name, etc. as defined in Cal. Penal Code Sec. 530.5(b), and uses that information for any unlawful purpose is guilty of a public offense. Identity theft is the fastest growing crime in the United States. Every year about 15 million people become victims. Everyone is vulnerable. Skilled identity thieves use a variety of methods to steal your personal information. These include the following:

- Dumpster diving. They rummage through trash looking for bills and other paper with your personal information on it.
- Skimming. They steal credit- or debit-card numbers with a special storage device when processing your card.
- Phishing, Spear Phishing, Smishing, Vishing, and Whaling. These are defined and tips for dealing with them are suggested in the section on Internet Fraud and Other Crimes in the SDPD paper entitled Cyber Security at **www.sandiego.gov/police/pdf/crimeprevention/CyberSecurity.pdf**.
- Changing your address. They divert your billing statements to another location by completing a change-of-address form.
- Stealing. They steal wallets, purses, mail (credit card and bank statements, pre-approved credit offers, new checks, tax information, etc.), employee personnel records, etc.

An enormous amount of information is available on various identity theft issues. Much of this is summarized in this paper, which contains tips for minimizing risk, things to do if you become a victim or are notified of a security breach involving personal information, links to a few other websites that deal with preventing identity theft, etc. A comprehensive set of links to the websites of a wide range of government agencies and nonprofit organizations that deal with these issues is on the Consumer Federation of American's website at **www.idtheftinfo.org**. It contains links that deal with consumer, business, and victim resources, shopping for identity theft services, statistics and studies, etc.

PROTECTING PERSONAL INFORMATION

The Basics

Some of the things you can do to minimize your risk of identity theft are listed below.

- Give out credit or debit card, bank account, and other personal information only when you have initiated the contact or know and trust the person you are dealing with. Beware of e-mail or telephone calls designed to obtain personal information. An example of this is a call from someone claiming to be from your local election board who asks for your SSN or other personal information to confirm your voter registration. These calls often occur prior to a big election.
- Put unique, strong passwords on all your online accounts and computing devices. Avoid using easily remembered numbers or available information like mother's maiden name or date of birth. Passwords should have more than eight characters, with at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words or easily-remembered phrases is recommended, e.g. Johnhave3dawgs! Hackers can run a program that goes through the entire dictionary very quickly and crack any password which can be found in it. They can also use grammar rules to crack long passwords, especially those with pronouns. So use bad grammar and nouns. For maximum security you should use randomly generated characters. You can test your passwords and get advice on creating strong ones at **www.microsoft.com/protect/yourself/password/checker.mspx**.
- Select password reset questions whose answers cannot be found online or from other research tools. Don't compromise a strong password with an easily answered reset question like: What is your mother's maiden name?
- Memorize your passwords. Don't carry them in your purse or wallet.
- Keep personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home.
- Make sure that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier's disk.
- Protect you health insurance cards like you would your credit or debit cards. If asked for your policy numbers or any other personal information in a doctor's office, make sure no one else is near enough to hear or see them.
- Protect your Medicare card number as you would your SSN. Don't give it to anyone who offers free medical equipment or services, or says they are from the government and then requests your number. And don't let anyone borrow or pay to use your Medicare card. That's foolish and illegal.
- Shred or tear up any documents with personal or financial information before throwing them in the trash. Use a cross-cut shredder. Or go paperless by signing up for electronic delivery.
- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.
- Omit any information that is not explicitly requested or required on forms, applications, surveys, etc. Information on them may be sold and become publicly available.
- Assume that anything placed on social networking websites will be publicly available. Do not post personal or sensitive information, or photos. And use appropriate security settings for anything you do post.
- Opting out of the services provided by data vendors can be time consuming and not always possible. There are hundreds websites that can be used to find addresses, phone numbers, civil and criminal court records, birth and death records, genealogy, etc. These include personal information aggregators like Spokeo that collect and sell public information from all these sources and social networks. Even if you hire a reputation manger to do this, public information will remain available online. You need to find the original source of the information and remove it there, which also may not be possible.

Using Credit and Debit Cards

- Use a credit card if at all possible. Don't use a debit card. If something goes wrong your bank account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. Even if your bank offers a fraud guarantee it is not obligated to restore your funds for at least two weeks while it investigates. If have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong. Or get an ATM-only card.
- Never loan your card to anyone.
- Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
- Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won't have access to the number.
- Notify your credit card companies and financial institutions in advance of any address or phone number changes.
- Bring home all card receipts and match them against your monthly statements. Look for charges you didn't make.
- Dispose of card receipts at home. Never toss them in a public trash container.
- Call the credit card company or bank involved if a new credit card you applied for hasn't arrived in a timely manner.
- Monitor the expiration dates of your cards and contact the card issuer if new cards are not received before your card expires.
- Report all lost or stolen cards immediately and request cards with new numbers. In this case the federal Truth in Lending Act limits your liability to $50 of any charges made before you report your card lost or stolen. Contact the issuer if replacement cards are not received in a reasonable time.
- Sign and activate new cards promptly on receipt. Or write "See ID" on the signature line on the back of the card. Then a thief won't have your signature. A merchant will ask you for a picture ID to make sure you are the cardholder.
- Never put a card number on a post card or on the outside of a mailing envelope.
- Make sure only the last four digits of your card number show up on your receipts. Use of full card numbers on electronically printed receipts is prohibited by California law. (Note that the merchant copy can show the full credit card number.) Report non-complying businesses to the Methamphetamine Strike Force hotline at **(877) 662-6384**.
- Cancel accounts you don't use or need. Carry only the cards and identification you need when you go out.
- Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
- Ask your credit card company to stop sending blank checks.
- Have your name removed from lists supplied by the Consumer Credit Reporting Companies (Equifax, Experian, and TransUnion) to be used for pre-approved/pre-screened offers of credit or insurance. Call **(888) 567-8688** or go to **www.optoutprescreen.com** to do this.
- Don't let your card out of sight. A person taking it to a Point of Sale (POS) device might have a skimmer to steal the information on the magnetic strip, copy your card number and the 3-digit security number on the back of the card, or switch cards. If you do give your card to a waiter or other sales person, make sure you get your card back. And use a credit card instead of a debit card whenever possible. With the former you don't have to pay disputed charges. But with the latter it may take the bank about two weeks to restore the funds to your account.
- Make sure your bank and credit card companies have your latest home and cell phone numbers, and e-mail address so they can contact you quickly if they suspect fraud in your accounts.
- Put a dollar limit on credit and debit card transactions and withdrawals. And put a number limit on transactions and withdrawals on any day.
- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction.

Furthermore, the information is on the chip is not the same as that on the magnetic strip, and it cannot be used to create a functioning counterfeit version of the card. If you have a card with a RFID chip and don't want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.

- Beware of skimmers on self-checkout terminals at grocery stores, gasoline pumps, and other places where you might swipe your credit or debit card. Things to watch for are listed below under Using an ATM.

Protecting Your U.S. Passport

- Since August 2007 all passports issued by the U.S. State Department have a small contactless RFID computer chip embedded in the back cover. They are called "Electronic or e-passports." The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder, a unique chip identification number, and a digital signature to protect the stored data from alteration. Unauthorized reading of e-passports is prevented by the addition of a radio-frequency blocking material to their covers. The passports cannot be read until they are physically opened. Then there are protocols for setting up a secure communication channel and a pair of secret cryptographic keys in the chip to ensure that only authorized RFID readers can read the data on the chip.
- In July 2008 the U.S. State Department began issuing U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive that a passport book. It cannot be used for international travel by air. To increase speed, efficiency, and security at U.S. land and sea border crossings the card contains a RFID chip. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the card when it is not in use. Make sure you carry the card in the sleeve.

Protecting Your SSN

- Examine your Social Security Personal Earnings and Benefits Estimate Statement for possible fraud. You will receive it about three months before your birthday each year. Make sure the reported income on the statement is not higher than that on your records. Contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at **www.ssa.gov/org** about any differences.
- Provide your SSN only when it is required by a government agency, employer, insurance company, healthcare provider, or financial institution. Never provide it on a request by e-mail or phone call. In a recent case a man received a call from a person who claimed to be a jury coordinator and said that a warrant has been issued for his arrest because he failed to report for jury duty. When he protested that he never received a summons he was asked for his SSN and date of birth to verify the records. Caught off guard he provided this information. Instead he should have hung up realizing that court workers would never ask for a SSN or other personal information.
- In a variation of the above scam, the caller says that you've been selected for jury duty and asks you to verify your name and SSN. Remember, notification of jury duty is always done by mail.
- Never use your SSN for identification. Don't carry it or your Social Security card in your purse or wallet.
- Do not have your SSN or driver's license number printed on your checks. And never write your SSN on a check.
- Provide your driver's license or some other identification number when reporting a crime in which you are the victim. Do not provide your SSN. The crime report will be available to the defense if a suspect is prosecuted.

Managing Your Accounts

- Keep a record in a secure place of all your credit and debit card, and bank and investment account phone numbers for quick reference if identity theft occurs.
- Review your bank statements carefully. Match your checkbook entries against paid checks. Look for checks you didn't write.
- Never leave transaction receipts at bank machines or counters, trashcans, gasoline pumps, etc.

Carrying Personal Information in a Purse or Wallet

- Carry only a driver's license, cash, and one credit card. Don't carry blank checks or a checkbook. Don't carry anything with a PIN written on it.
- Keep a record of its contents. Photocopy both sides of your credit and debit cards and driver's license and keep them in a safe place at home.
- Don't carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card is a safe place at home.
- If you carry a wallet in a purse, keep credit or debit cards in separate compartment and not in your wallet.
- Don't carry personal information of your family members.
- Don't carry any account numbers or passwords.

Securing Mobile Devices

Smartphones, tablets, and other mobile devices are now as powerful and functional as many computers. Therefore is necessary to protect them just like you protect your computer or laptop. The following tips will help to safeguard your personal information:

- Use a strong password to protect your device. Use different passwords of each payment app.
- Lock your device when you're not using it. Even if you only step away for a few minutes, it's enough time for someone else to steal or destroy information in it. Use the security lockout feature so the device automatically locks after it's not in use for a certain period of time.
- Disconnect your device from the Internet when you aren't using it. The likelihood that attackers or viruses scanning the network for available devices will target you becomes much higher if your device is always connected.
- Keep software up to date. Install patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. Install them.
- Consider creating separate user accounts. If multiple people are using the device, someone else may accidentally access, modify, or delete your information. If you have the option, create different user accounts for each user and set the access and privileges for each account.
- Establish guidelines for usage. If multiple people using your device, especially children, make sure they understand how to use the device safely. Setting boundaries and guidelines will help protect your data.
- Back up your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. Regularly backing it up reduces the stress and consequences that result from losing important information.

Before Going Away on an Extended Trip

- Consider placing a security freeze on your credit reports. Go to the websites of Equifax, Experian, and TransUnion for their procedures and fees for placing and lifting freezes. Their addresses are: **www.equifax.com**, **www.experian.com**, and **www.transunion.com**, respectively. A freeze will stop these reporting companies from sharing your credit reports with any creditors or insurance companies. Thus anyone who might have stolen your identity will be unable to open new accounts in your name while you are gone because creditors will usually not open new accounts without credit reports. You can lift the freeze when you return.
- Alert your credit card companies about when, where, and how long you will be away. This will enable their fraud departments to stop charges if your card is used where you are not, and reduces the risk that charges made where you are going to be will not be accepted.

Using the Mail

- Deposit outgoing mail at a Post Office, in a blue U.S. Postal Service collection box, or give it directly to your mail delivery person. Put it in a collection box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Also, do not leave mail for pickups from personal curbside boxes or cluster box units.

- Pick up your mail as soon as possible after it arrives in your personal curbside box or cluster box unit. If this is not possible, have a trusted friend or neighbor collect your mail, especially if you are expecting a box of checks or a new credit or debit card.
- Consider having new checks mailed to your bank for collection to avoid possible theft from your mailbox.
- Use a locked mailbox and make sure the lock works.
- Investigate immediately if bills do not arrive when expected, you receive unexpected credit cards or account statements, you are denied credit for no apparent reason, and you receive call or letters about purchases you did not make.
- Report the non-receipt of expected valuable mail by calling the sender and the Postal Inspection Service as soon as possible.
- To reduce junk mail you can remove yourself from many national mailing lists by registering for the Direct Marketing Association (DMA) Mail Preference Service at **www.DMAchoice.org/register.php**. There you can stop catalogs, magazine offers, and other mail offers. You can also click on a link to manage prescreened credit offers. It will take you to **www.optoutprescreen.com**.

Using an ATM

- Use ATMs that are inside a store or a bank. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder's financial information from an ATM transaction. If you use an outside ATM, it should be well-lighted and under video surveillance.
- Get off your cell phone and be alert when using an ATM.
- Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. If something doesn't seem right, go to another machine.
- Some ATMs have flashing lights in the card slot. Their obscuration is a sign of tampering.
- Look to see if there is anything in the slot where you insert your ATM card. Thieves place a small, thin, hard-to-detect skimming device in the card slot to steal your PIN and other bank account information. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, turn it over to the local law enforcement agency as soon as possible with a note on where and when you removed it. Don't throw it away or keep it. Be aware that the criminals doing the skimming may be watching the ATM.
- Check for a false keypad that has been installed over the built-in one. False keypads stick out too far or look strange.
- Check the area around the machine for hidden cameras. To be safe shield your hand when entering your PIN so it can't be seen by anyone near you or by a hidden camera.
- If you use a debit card memorize your PIN and keep it secret. Don't write it down or keep it in your wallet or purse.
- Keep the customer-service phone numbers of your bank and credit-card company readily available. Call the appropriate number immediately if your card gets stuck in an ATM. Do not leave the ATM.
- Don't leave your transaction receipts at the ATM. Take them home and use them in balancing your account.
- Monitor your bank statements frequently and report any unauthorized activity immediately.

PROTECTING YOUR CHILD'S IDENTITY

- Provide your child's SSN only when it is required by a government agency or financial institution. Never provide it for identification.
- Carry your child's SSN or card in your purse or wallet only when you know you will need it.
- Teach your child never to give out personal information over the phone or on the Internet.
- Check to see if your child has a credit report. There should not be one unless someone has applied for credit using your child's SSN number. No minor should have a credit report. At a Federal Trade Commission (FTC)-sponsored forum on child-centric fraud in July 2011 it was estimated that more than 140,000 American children become victims of identity theft each year. By various means thieves obtain children's SSNs and sell these genuine numbers to persons with poor credit ratings who obtain credit cards, make extensive purchases, and don't pay their bills. If this happens you should contact the credit card companies and the three nationwide consumer credit reporting bureaus immediately.

- Watch your child's mail for credit card applications, bills, or bank statements. They are signs that someone has started a credit history in your child's name.
- Request that banks in which your child has an account remove his or her name from marketing lists.
- Report any suspected identity theft to the three nationwide consumer credit reporting bureaus and obtain copies of any credit reports in your child's name and SSN. If your child does have a credit report, ask to have all accounts, application inquiries, and collection notices removed immediately. Tell the credit issuer that the account is in the name of your minor child who by law isn't permitted to enter into contracts.
- Take advantage of your rights under the Children's Online Privacy Protection Act (COPPA). This law and FTC mandates under it require websites and mobile apps to get parental consent before collecting and sharing information from children under 13 years old. This includes photos, videos, geolocation, and tracking tools such as cookies that use Internet Protocol addresses and mobile device IDs to follow a child's web activities across multiple apps and sites. COPPA covers sites and apps designed for children under 13 and general-audience sites and apps that know certain users are under 13. It protects information that sites and apps collect upfront and information that children give out or post later. It also requires these sites and apps to post a privacy policy that provides details about the kind of information they will collect and what they might do with the information. You should: (1) know your rights, (2) be careful with your permission, (3) check out the sites your children visit and apps they use, (4) review the sites' and apps' privacy policies, (5) contact the site of app if you have any questions about its privacy policy, and report any site or app that breaks the rules to the FTC at **www.ftc.gov/complaint**. For answers to frequently asked questions about the Children's Online Privacy Protection Rule go to **www.ftc.gov/privacy/coppafaqs.shtm**.

BUYING IDENTITY THEFT PROTECTION

- You cannot buy absolute protection against identity theft. Beware of any such claims, especially regarding prevention of misuse of existing credit-card accounts, theft of medical records, and theft of personal information from employer's personnel files. For example, fraud alerts and credit freezes just make it more difficult for identity thieves to open new accounts in your name. These make up a small fraction of all identity theft incidents.
- Before signing up for protection, be sure to understand what services are provided, what protections they afford, and how the personal information you provide is protected.
- Identity theft protection companies offer services that range from placing and renewing fraud alerts and credit freezes on your credit reports to monitoring your credit reports for recent activities, helping you rebuild your identity if is stolen, reimbursing you for losses due to identity theft, removing your name from mailing lists of pre-screened offers of credit or insurance, etc.
- In buying identity theft protection you will be paying for many things you can do for yourself at no cost. These include placing and renewing fraud alerts and credit freezes, obtaining annual credit reports, and removing your name from mailing lists. These protective measures are discussed below.

CHECKING FOR POSSIBLE IDENTITY THEFT

- Obtain free copies of your credit reports from the three nationwide consumer credit reporting bureaus (Equifax, Experian, and TransUnion) by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**. This is the ONLY source of free reports authorized under Federal law. You can get one free report annually from each bureau. Stagger your requests to obtain one every four months. That way you can monitor your credit during the year. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit. Contact the reporting bureau immediately if you see any inaccuracies. These bureaus may also try to sell you credit monitoring products or services for a fee. The FTC requires that any advertising for such products or services be delayed until after you get your free credit reports.
- Be aware that if you order a free credit report from an unauthorized website such as **freecreditreport.com** you will be given a free limited-time trial membership in its credit monitoring service that will provide daily monitoring of your credit reports, alert notices of key changes, bi-monthly credit scores, etc. If you don't cancel this membership you will be charged a fee for each month that you remain a member. Before becoming a member you need to understand exactly what protection and services it will and will not provide, and whether you need the additional protection.

- These websites are required to print a disclosure that states the following at the top of each page that mentions free credit reports: "THIS NOTICE IS REQUIRED BY LAW. Read more at **www.FTC.gov**. You have the right to a free credit report from **www.AnnualCreditReport.com** or **(877) 322-8228,** the ONLY authorized source under federal law." They are also required to include a clickable button to "Take me to the authorized source" and clickable links to **www.AnnualCreditReport.com** and **www.FTC.gov**. However, neither of these requirements is enforced by the FTC so they don't appear on websites that advertise free credit reports**.**
- If you find an error in a report you should submit a dispute directly to the credit reporting bureau. Its e-mail address, mailing address, and phone number should be on the credit report. Credit bureaus are required to respond within 30 days. They will contact the lender that provided the information under dispute. If a fix is made the lender will contact all three credit bureaus. When the investigation is complete must provide written results and a free copy of your report. You should also contact the lender and ask that they update the credit bureaus with correct information. If you are not satisfied with the results of these investigations you should file a complaint with the Consumer Financial Protection Bureau, the federal agency that enforces the rules for credit reporting and monitors compliance by the credit bureaus. You can do this online at **www.ConsumerFinance.gov/Complaint** or by phone at **(855) 411-2372**. In any case don't pay a Credit Repair Organization (CRO) to handle your dispute. It can't do anything more than what you can do. And if you encounter a CRO that promises to remove negative items from your credit reports it is safe to assume it's a scam, as discussed under Credit Repair in the SDPD paper on Fraud Prevention at **www.sandiego.gov/police/pdf/crimeprevention/FraudPrevention.pdf**.
- Check your medical bills and health insurance statements to make sure the dates and types of services match your records. Read every letter you get from your insurer, including those that say "this is not a bill." If you see a doctor's name or date of service that isn't familiar, call the doctor and your insurer.
- Once a year request a list of all benefits paid in your name by your health insurer. If the thief has changed your billing address you would not be receiving any bills or statements.
- These checks are critical in detecting synthetic identity theft, which is now the prevalent kind of identity theft. In it the thieves create new identities by combining real and fake identifying information to establish new accounts with fictional identities. In typical case a thief may use your SSN and combine it with another name and address. This combination won't show up on your credit reports. The credit reporting bureaus may create a new file for it or a subfile under your file. Although synthetic identity theft mainly hurts creditors, you can be affected and should do the following in addition to the checks listed above:
  - Look out for suspicious mail sent to your home address with someone else's name on it. It may be a change-of-address notice, a credit offer, or a statement for an account you didn't open.
  - Contact your credit-card company or bank if any expected mail does not arrive on time.
  - If you are denied credit, make sure the creditor's decision is based on your identity and personal credit information, and not someone else's.
  - Consider buying an identity theft protection service that will monitor your personal credit information, scour the Internet for unauthorized use of your credit and debit cards and SSN, and alert you if any changes are detected.
  - Be prepared to deal with debt collectors for purchases you did not make. They can find you in a SSN search.

IF YOU BELIEVE YOU MAY BECOME VICTIM

If you believe your personal information has been compromised, e.g., if you wallet is lost or stolen, don't wait until you become a victim to report the loss or theft to the FTC, SSA, IRS, and other agencies that might be involved. And contact one of the three credit reporting bureaus to have an initial fraud alert placed on your credit reports. The company you call is required to notify the other two. Their phone numbers are: **(800) 525-6285** for Equifax, **(888) 397-3742** for Experian, and **(800) 680-7289** for TransUnion. This fraud alert is free and is good for 90 days. It can be renewed after that. It places a signal on your credit reports to warn potential creditors that they must verify your identity before issuing credit. It also allows you to order one free copy of your credit report from each of the three credit reporting companies. This alert may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts.

Because there is so much income tax fraud, contact the IRS Identity Protection Specialized Unit (IPSU) at **(800) 908-4490** if you believe your SSN has been compromised. (In 2011 the IRS detected about one million fraudulent tax returns claiming $6.5 billion in refunds, and may have delivered more that $5 billion in refund checks to

identity thieves. It also estimated that there might be another 1.5 million undetected cases of thieves seeking refunds after assuming the identity of a dead person, child, or someone else who normally would not file a tax return.) The IPSU will suggest that you file a completed IRS Form 14039, Identity Theft Affidavit. This will authorize the IRS to put a marker on your account that will help it protect you from identity theft and resolve future identity theft issues.

IF YOU BECOME A VICTIM

File a police report as soon as possible if you become a victim of identity theft, i.e., when someone has obtained your personal information and used it for an unlawful purpose. Call the SDPD non-emergency number, **(619) 531-2000** or **(858) 484-3154**, and give the dispatcher a description of the theft. An officer will call to take a full report, including any information you may have on suspects and witnesses, and give you a case number. Then do the following:

- Set up a folder where you can keep a log of all your reports and supporting documents, and contacts and their phone numbers. You will need to refer to the case number when you have contacts with any business or law enforcement agencies concerning your case.
- Contact the FTC to report the theft. Its Identity Theft Hotline is **(877) 438-4338**. Or visit its website at **www.ftc.gov/idtheft**. The FTC is the federal clearinghouse of complaints of victims of identity theft. It helps victims by providing information to resolve financial and other problems that could result from identity theft. Its booklet entitled *Take Charge: Fighting Back against Identity Theft* deals with bank accounts and fraudulent withdrawals, bankruptcy fraud, investment fraud, phone fraud, and other specific problems. It also describes the immediate steps victims should take and ways to minimize recurrences.
- Report the theft to the fraud unit of Equifax at **(800) 525-6285**, Experian at **(888) 397-3742**, or TransUnion at **(800) 680-7289** and request an extended fraud alert be placed on your credit reports. The company you call is required to inform the other two. Extended fraud alerts are free and good for seven years. For this you will have to provide a copy of a police report and proof of your identity. You may also have to fill out a request form. When you request an extended fraud alert you are entitled to two free copies of your credit reports within 12 months from each of the three credit reporting bureaus. Review them carefully and look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Also, your name will also be taken off marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list. This fraud alert permits some creditors to get your report as long as they take steps to verify your identity, which may include contacting you in person. Like an initial fraud alert, an extended alert may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts.
- An alternative to an extended fraud alert is a credit freeze. A freeze generally stops all access to your credit reports, but like a fraud alert, it may not stop misuse of your existing accounts or other types of identity theft. Where fraud alerts are governed by federal law, the availability of credit freezes depends on state law and reporting bureau policies. And they are not free.
- Alert your banks of the theft and request new account numbers with new checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the theft.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports. Also change your PINs and passwords.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft. If you still want a charge account, request a new number.
- Report the theft to the IRS IPSU at **(800) 908-4490** if your SSN is involved. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. You should also go to **www.irs.gov/privacy/article/0,,id=186436,00.html** for answers to the following questions. How to protect yourself from identity theft? What are indications that your identity has been stolen and how to report it to the

IRS? Where else should you report it? What is the IRS doing to prevent identity theft and help victims? What other resources are available to help prevent identity theft?

- Contact the SSA on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at **www.ssa.gov/oig** if your SSN is compromised.
- Call the U.S. Secret Service at **(619) 557-5640** if the crime involves counterfeit credit cards or computer hacking.
- Contact the California DMV Fraud Hotline at **(866) 658-5758** to report the theft and see if another driver's license has been issued in your name.
- Notify the U.S. Postal Inspector if your mail has been stolen or tampered with. Its number is **(626) 405-1200**. Or report it online at **http://postalinspector.uspis.gov**.
- In the case of medical identity theft request a copy of your current medical files from each health care provider, and request that all false information be removed from your medical and insurance files. Enclose a copy of the police report with your requests. For more information things to do if you are a victim of medical identity theft or concerned about it go the World Privacy Forum's website at **www.worldprivacyforum.org/ medicalidentitytheft.html**.
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any theft that involves Medicare.
- If you are contacted by a collector for a debt that resulted from identity theft, send the debt collector a letter by certified mail, return receipt requested, stating that you did not create the debt and are not responsible for it. Include a copy of the police report you filed for the identity theft crime and a completed copy of the FTC's Identity Theft Victim's Complaint and Affidavit. It can be downloaded from its website at **www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf**. Also write in your letter that you are giving notice to a claimant under California Civil Code Sec. 1798.93(c)(5) that a situation of identity theft exists.
- Call the SDPD Economic Crimes Section at (619) 531-2545 and talk to the investigator if you have any questions about your case, or have more information to provide.
- Other things you should do as a victim are in the Identity Theft Victim Checklist on the website of the California Office of Privacy Protection at **www.privacy.ca.gov/consumers/cis3english.pdf**. It's website at **www.privacy.ca.gov** contains additional information on identity theft resources, credit file security freezes, SSN protection, etc.

Another useful website is that of the Identity Theft Resource Center (ITRC) at **www.idtheftcenter.org**. It contains information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft. It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, and answers to frequently asked questions. Its toll-free victim-assistance number is **(888) 400-5530**.

IF YOU ARE NOTIFIED OF A SECURITY BREACH INVOLVING PERSONAL INFORMATION

Most states now have security breach notification laws under which a person whose personal information is compromised must be notified of the breach. The California Breach Notification Law is in Civil Code Sections 1798.29, 1798.82, and 1798.84. The first applies to state government agencies; the other two apply to any person or business doing business in the state. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: SSN; driver's license or California Identification Card number; financial account, credit card, or debit-card number along with any PIN or other access code required to access the account; medical information; or health insurance information. You should do the following for each and also be alert for possible spear phishing as defined above under Internet fraud and other crimes:

- SSN. Put an initial fraud alert on your credit reports at Equifax, Experian, and TransUnion, and order copies of your reports. Review them carefully and file a police report if you find anything suspicious. If you don't find anything suspicious at first, renew the fraud alert and check your credit reports periodically. Also report the loss to the FTC, IRS, and SSA.
- Driver's License or California Identification Card number. Call the DMV Fraud Hotline to report the incident.
- Financial account numbers. Call the institution to request new account numbers and PINs. And put new passwords on your accounts.
- Medical or health insurance information. Review your explanation of benefits statements and contact your insurer if you see any services you did not receive.

For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse's website at **www.privacyrights.org**.